CLAIMS

1. A method for authenticating a user of a first terminal in a communication system,

characterized in that the method comprises the steps of:

setting up a first logical channel via a communication network between a first terminal and a service provider; and

identifying the identity of the user of the first terminal after the first logical channel set up via a second logical channel other than the established first logical channel between the service provider and the first terminal prior to providing any services to the user of the first terminal.

2. The method according to claim 1, characterized in that the method further comprises the steps of:

sending a user identification request from the service provider to the first terminal via the second logical channel while the first logical channel exists between the first terminal and the service provider;

receiving the user identification request with the first terminal while the first logical channel exists;

digitally signing the request;

sending the signed request with the first terminal via the second logical channel;

authenticating the user of the first terminal and verifying the digital signature; and

providing the user with services provided by the service provider via the first logical channel.

3. The method according to claim 1, characterized in that the method further comprises the steps of:

sending a user identification request for the user of the first terminal from the service provider to a second terminal via the second logical channel while

the first logical channel exists between the first terminal and the service provider;

receiving the user identification request with the second terminal while the first logical channel exists;

digitally signing the request;

sending the signed request with the second terminal via the second logical channel;

authenticating the user of the second terminal and verifying the digital signature; and

providing the user of the first terminal with services provided by the service provider via the first logical channel.

4. The method according to claim 1, characterized in that the method further comprises the steps of:

sending a user identification request for the user of the first terminal from the service provider to a second terminal via the second logical channel, the user identification request comprising also a challenge;

receiving the user identification request comprising the challenge with the second terminal;

digitally signing the request comprising the challenge;

sending the signed request with the second terminal via the second logical channel;

providing the user of the first terminal with the challenge with the second terminal;

providing the service provider with the challenge acquired from the user of the second terminal;

comparing the challenge in the signed message from the second terminal and the challenge provided by the user of the first terminal; and if the challenges are equal,

authenticating the user of the second terminal and verifying the digital signature; and

providing the user of the first terminal with services provided by the service provider via the first logical channel.

5. The method according to claim 1, 2, 3 or 4, characterized in that the first and/or second logical channel refers to a packet switched connection.

6. The method according to claim 1, 2, 3 or 4, characterized in that the first and/or second logical channel refers to a circuit switched connection.

7. The method according to claim 1, 2, 3 or 4, characterized in that the method further comprises the step of:

arranging a security gateway forming an interface towards the first and/or second terminal.

8. The method according to claim 7, characterized in that the method further comprises the steps of:

identifying the service provider with the security gateway;

sending a user identification request from the service provider to the security gateway;

sending the user identification request from the security gateway to the first terminal via the second logical channel;

receiving the identification request with the first terminal;

digitally signing the request;

sending the signed request to the security gateway via the second logical channel;

retrieving a certificate related to the user of the first terminal;

authenticating the identity of the user of the first terminal and verifying the digital signature; and

providing the user of the first terminal a service provided by the service provider via the existing first logical channel.

9. The method according to claim 7, characterized in that the method further comprises the steps of:

identifying the service provider with the security gateway;

sending a user identification request of the user of the first terminal from the service provider to the security gateway;

sending the user identification request from the security gateway to a second terminal via the second logical channel;

receiving the user identification request with the second terminal;

digitally signing the request;

sending the signed request to the security gateway via the second logical channel;

retrieving a certificate related to the user of the second terminal;

authenticating the identity of the user of the second terminal and verifying the digital signature; and

providing the user of the first terminal a service provided by the service provider via the existing first logical channel.

10. The method according to claim 2, 3, 4, 8 or 9, characterized in that the method further comprises the step of:

encrypting the user identification request sent to the first and/or second terminal using symmetric or asymmetric encryption; and

encrypting the signed request sent from the first and/or second terminal using symmetric or asymmetric encryption.

11. The method according to claim 8 or 9, characterized in that the method further comprises the step of:

encrypting the signed user identification request sent to the security gateway using symmetric or asymmetric encryption.

12. The method according to claim 8 or 9, characterized in that the method further comprises the steps of:

retrieving with the security gateway a certificate related to the user of the first and/or second terminal;

creating and sending a validating message to the service provider; and

validating the user of the first and/or second terminal with the service provider based on the validating message and validating information.

13. The method according to claim 8 or 9, characterized in that the method further comprises the steps of:

retrieving with the security gateway validation information comprising at least a certificate related to the user of the first and/or second terminal;

authenticating the identity of the user of the first and/or second terminal with the security gateway based on the validation information; and

sending a positive validation message to the service provider if the result of the validation was positive.

14. The method according to claim 1, characterized in that if the first logical channel fails during the validation procedure, the method further comprises the steps of:

creating a challenge;

encrypting the challenge with the public encryption key of the user of the first terminal;

sending the encrypted challenge to the first terminal;

decrypting the encrypted challenge in the first terminal;

setting up a new logical channel to the service provider;

providing the service provider with the decrypted challenge; and if the challenge is acceptable,

providing the user of the first terminal via the logical channel with a service provided by the service provider.

15. The method according to claim 14, characterized in that the method further comprises the step of:

sending the encrypted challenge to the first terminal via a security gateway.

16. A system for authenticating a user of a first terminal in a communication system, the system comprising:

a communication network (NET),

a first terminal (DTE) associated with the communication network (NET),

a service provider (SP) associated with the communication network (NET),

a certificate service provider (CA),

characterized in that the system further comprises:

sending means (SM) for sending a user identification request to the first terminal (DTE) or a second terminal (DTE2); and

identifying means (ID) for identifying the identity of the user of the first terminal (DTE) after a first logical channel has been set up via a second logical channel other than the established first logical channel between the service provider and the first terminal (DTE) prior to providing any services to the user of the first terminal (DTE) based on the informa-

tion provided by the certificate service provider (CA).

17. The system according to claim 16, characterized in that the system further comprises:

a security gateway (GW) in connection with the service provider (SP) and certificate service provider (CA).

18. The system according to claim 17, characterized in that the security gateway (GW) is managed by the service provider (SP).

19. The system according to claim 17, characterized in that the security gateway (GW) is managed by a third party.

20. The system according to claim 16, characterized in that said sending means (SM) are arranged in the service provider (SP).

21. The system according to claim 16 or 17, characterized in that said sending means (SM) are arranged in the service provider (SP) and security gateway (GW).

22. The system according to claim 16 or 17, characterized in that said identifying means (ID) are arranged in the service provider (SP) and/or security gateway (GW).

23. The system according to claim 16, characterized in that the service provider (SP) comprises:

first encrypting means (EN1) for encrypting information; and

first decrypting means (DE1) for decrypting information.

24. The system according to claim 17, characterized in that the security gateway (GW) comprises:

second encrypting means (EN2) for encrypting information; and

second decrypting means (DE2) for decrypting information.

25. The system according to claim 16, characterized in that the first terminal (DTE) and/or second terminal (DTE2) comprises:

third encrypting means (EN3) for encrypting information; and

third decrypting means (DE3) for decrypting information.

26. The system according to claim 20 or 21, characterized in that said sending means (SM) are arranged to send a challenge to the first terminal (DTE) in the event that the logical channel set up between the first terminal (DTE) and service provider (SP) fails.

27. The system according to claim 20 or 21, characterized in that said sending means (SM) are arranged to send a challenge to the second terminal (DTE2).

28. The system according to any of the claims 16 - 27, characterized in that the communication network is a GSM network.

29. The system according to any of the claims 16 - 27, characterized in that the communication network is a GSM network with the GPRS feature.

30. The system according to any of the claims 16 - 27, characterized in that the communication network is an UMTS, a CDMA, a WCDMA, an EDGE, a Bluetooth, or a WLAN network.